Regio Rivierenland

BLAD GEMEENSCHAPPELIJKE REGELING

Nr. 275

26 mei

2016

Officiële uitgave van gemeenschappelijke regeling
Regio Rivierenland.

Regeling gebruik e-mail, internet en social media Regio Rivierenland

Het dagelijks bestuur van Regio Rivierenland,

gelet op het feit dat Regio Rivierenland medewerkers e-mail- en internetfaciliteiten ter beschikking stelt om met behulp daarvan hun werkzaamheden uit te voeren;

gelet op het feit dat aan het gebruik van e-mail en internet risico's zijn verbonden, zoals beschadiging van het netwerk door virussen, het uitlekken van bedrijfsgeheimen en het in diskrediet brengen van de goede naam van Regio Rivierenland;

gelet op de wenselijkheid de regeling voor het gebruik van e-mail en internet te actualiseren en het gebruik van social media hieraan toe te voegen;

gelet op het bepaalde in de Wet bescherming persoonsgegevens;

gelet op het integriteitbeleid van Regio Rivierenland zoals vastgesteld op 18 juni 2014;

gelet op de instemming van de Ondernemingsraad d.d. 9 oktober 2014 en 20 april 2016 ;

besluit
vast te stellen de navolgende Regeling gebruik e-mail, internet en social media Regio Rivierenland

Artikel 1 Begripsbepalingen

In deze regeling wordt verstaan onder:
Bestand: Elk, al dan niet geautomatiseerd, gestructureerd geheel van persoonsgegevens, ongeacht of dit geheel van gegevens gecentraliseerd is of verspreid is op een functioneel of geografisch bepaalde wijze, dat volgens bepaalde criteria toegankelijk is en betrekking heeft op verschillende personen.
Cbp: College bescherming persoonsgegevens: het College als bedoeld in artikel 51 Wbp.
Elektronische communicatiemiddelen: e-mail- en/of internetfaciliteiten.
E-mailfaciliteiten: De door of namens Regio Rivierenland aan medewerkers ter beschikking gestelde e-mailfaciliteiten.
Internetfaciliteiten: De door of namens Regio Rivierenland aan medewerkers ter beschikking gestelde internetfaciliteiten.
Medewerker: De ambtenaar bedoeld in artikel 1:1, eerste lid, onder a van de CAR- UWO;
Onrechtmatig gebruik dan wel misbruik van de elektronische communicatiemiddelen: een doen of nalaten in strijd met dit reglement of andere wet- en regelgeving of een inbreuk op een recht.
Persoonsgegevens: Elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon in de zin van de Wbp.
Social Media: De benaming voor de internet-platformen waar gebruikers de inhoud bepalen. Voorbeelden zijn weblogs, forums, wiki's en sociale netwerken.
Verantwoordelijke: het Dagelijks Bestuur van Regio Rivierenland).
Verwerken van persoonsgegevens: Elke handeling of geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval; het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens.
Wbp : Wet bescherming persoonsgegevens

Artikel 2 Reikwijdte

1. Deze regeling is van toepassing op het verwerken van persoonsgegevens inzake het gebruik van elektronische communicatiemiddelen.
2. Deze regeling geldt voor medewerkers in dienst van Regio Rivierenland en personen die werkzaamheden voor Regio Rivierenland verrichten, anders dan in ambtelijk dienstverband.

Artikel 3 Doeleinden

1. De verwerking van persoonsgegevens inzake het gebruik van de elektronische communicatiemiddelen heeft de volgende doeleinden:
    a. Het verkrijgen van inzicht in de mate van gebruik van de elektronische communicatiemiddelen;

   b. Het voorkomen van onrechtmatig gebruik dan wel misbruik van de elektronische communicatiemiddelen.

2. De omvang van de controle ter voorkoming van het genoemde in het eerste lid sub b, moet in redelijke verhouding staan tot het doel van de controle.

Artikel 4 Gebruik social media

1. Algemene berichtgeving over Regio Rivierenland wordt altijd via de communicatieadviseur in diverse (social) media geplaatst. Medewerkers mogen uitsluitend gebruik maken van social media indien het werk er niet onder lijdt. Afhankelijk van de functie van een medewerker kan het gebruik van social media meer of minder gewenst zijn. Leidinggevende en medewerker maken hierover concrete afspraken
   a. De medewerker mag kennis en andere waardevolle informatie delen, mits die informatie niet vertrouwelijk is en Regio Rivierenland niet schaadt.
   b. Medewerker publiceert niet ongevraagd vertrouwelijke of andere merkgebonden informatie. Voor het publiceren van gesprekken wordt eerst toestemming gevraagd aan de sprekers, de leidinggevende of de daarvoor verantwoordelijke afdeling of persoon.
   c. Medewerkers mogen geen vertrouwelijke of schadelijke informatie verstrekken over klanten, partners of leveranciers zonder hun voorafgaande goedkeuring. Hierin wordt geen onderscheid gemaakt tussen informatie over het product en de persoon of het bedrijf.
   d. Medewerkers dienen extra voorzichtig te zijn bij het publiceren over, of in discussie gaan met, een klant, partner of leverancier. Verkeerd opgevatte of slecht onderbouwde stukken, kunnen direct nadelige gevolgen hebben.
   e. De medewerker die publiceert op een website (of andere social media) anders dan die van Regio Rivierenland over een onderwerp dat wel te maken kan hebben met Regio Rivierenland, maakt kenbaar dat zij op persoonlijke titel publiceren. Als medewerker namens Regio Rivierenland spreekt, vermeldt hij de organisatie en zijn functie.

2. Directeur(en) en Secretaris hebben een bijzondere verantwoordelijkheid bij het gebruik van social media. Voor deze functies geldt vaak dat iemand altijd wordt gezien als vertegenwoordiger van Regio Rivierenland – ook als hij/zij een privé- mening verkondigt. Op grond van de positie moeten zij nagaan of zij op persoonlijke titel kunnen publiceren.
3. De medewerker is persoonlijk verantwoordelijk voor de inhoud die hij, voor zover dat niet tot de functie behoort, publiceert op blogs, wiki's, fora en andere media die gebaseerd zijn op user-generated content. Medewerker is er zich van bewust dat wat hij publiceert voor langere tijd openbaar zal zijn, met gevolgen voor zijn privacy.
4. Sociale omgangsvormen gelden online op gelijke wijze als offline. Laster, beledigingen en andere ongepaste uitingen zijn niet geoorloofd. De privacy van anderen wordt gerespecteerd.
5. Wanneer een online discussie dreigt te ontsporen, of al ontspoord is, neemt de medewerker direct contact op met de leidinggevende en de verantwoordelijke afdeling/persoon. In overleg wordt de te volgen strategie bepaald.
6. Bij de geringste twijfel over een publicatie of over de raakvlakken met Regio Rivierenland treedt de medewerker in overleg met zijn leidinggevende of de daarvoor verantwoordelijke afdeling/persoon.
7. Blogs en sociale netwerken die worden gepubliceerd onder naam van werkgever moeten worden gebruikt op een manier die waarde toevoegt aan de bedrijfsdoelstellingen.
8. Wanneer medewerker op een persoonlijke blog over het werk schrijft, dient een disclaimer[1] te worden opgenomen waarin staat dat dit blog een persoonlijk standpunt weergeeft en dat dit niet overeen hoeft te komen met dat van de organisatie.

[1] "de hier gepubliceerde uitingen vertegenwoordigen uitsluitend mijn persoonlijke meningen en opvattingen en komen niet noodzakelijkerwijs overeen met die van Regio Rivierenland".

Artikel 5 Voorkomen onrechtmatig gebruik dan wel misbruik

Regio Rivierenland neemt maatregelen in technische zin ter voorkoming van onrechtmatig gebruik dan wel misbruik van de elektronische communicatiemiddelen. In dit verband kan Regio Rivierenland onder meer de toegang tot bepaalde sites beperken.

Artikel 6 Verantwoordelijkheden en beheer

1. Het Dagelijks Bestuur van Regio Rivierenland treft de nodige maatregelen voor de juistheid en nauwkeurigheid van de persoonsgegevens.
2. Het Dagelijks Bestuur van Regio Rivierenland draagt zorg voor technische en organisatorische maatregelen om persoonsgegevens te beveiligen tegen verlies en tegen onrechtmatige verwerking van de gegevens.
3. Het Dagelijks Bestuur van Regio Rivierenland wijst één of meerdere systeembeheerders aan die belast zijn met het beheer van de bestanden. De systeembeheerders zijn verplicht tot geheimhouding van de gegevens waarover zij in dit verband beschikken.

Artikel 7 Gebruik elektronische communicatiemiddelen

1. Regio Rivierenland kan het recht tot het gebruik van (een deel van) het internet toestaan, maar ook altijd weer intrekken. Zonder dat recht is gebruik van (een deel van) het internet niet toegestaan.
2. Medewerkers gebruiken de elektronische communicatiemiddelen primair voor het uitvoeren van de aan hen door Regio Rivierenland opgedragen taken.
3. Incidenteel privégebruik van de elektronische communicatiemiddelen door medewerkers is toegestaan mits dit gebruik in overeenstemming is met deze regeling en dit gebruik in geen geval storend is voor dan wel ten koste gaat van het uitvoeren van de aan hen door Regio Rivierenland opgedragen taken.
4. Het is medewerkers niet toegestaan met behulp van de e-mailfaciliteiten:
   a. Berichten anoniem of onder een fictieve naam te versturen;
   b. Kettingbrieven te versturen;
   c. Pornografisch materiaal te versturen of op te vragen;
   d. Dreigende, seksueel intimiderende, racistische of discriminerende opmerkingen te maken;
   e. Illegale software te verzenden of op te vragen;
   f. Bestanden zonder voorafgaande toestemming van de systeembeheerder(s) te verzenden of op te vragen waarvan medewerker redelijkerwijs moet aannemen dat deze te omvangrijk zijn.

5. Het is medewerkers niet toegestaan met behulp van de internetfaciliteiten:
   a. Bewust internetsites die pornografisch, dan wel racistisch materiaal bevatten te bezoeken;
   b. Mee te doen in chat-sessies, behalve wanneer deze georganiseerd zijn door Regio Rivierenland;
   c. Online te gokken;
   d. software te downloaden dan wel zonder voorafgaande toestemming van de systeembeheerder(s) bestanden te downloaden waarvan medewerker redelijkerwijs moet aannemen dat deze te omvangrijk zijn;
   e. Zich ongeoorloofd toegang te verschaffen tot niet openbare bronnen op het internet.

6. Indien medewerkers ongevraagd informatie met een dreigend, beledigend, sexueel getint, racistisch dan wel discriminerend karakter aangeboden krijgen, dienen deze dit te melden aan hun leidinggevenden.
7. Medewerkers zullen bij het gebruik van de elektronische communicatiemiddelen de nodige zorgvuldigheid betrachten en de integriteit[2] en goede naam van Regio Rivierenland waarborgen.

[2] Zie het integriteitbeleid Regio Rivierenland, inclusief de onderliggende regelingen, op het intranet van Regio Rivierenland

Artikel 8 Vastlegging

1. Elektronisch vastleggen van persoonsgegevens geschiedt (automatisch) door de door Regio Rivierenland ingezette sofware.
2. De vastlegging beperkt zich tot de gegevens die noodzakelijk zijn voor de doeleinden van de verwerking als bedoeld in artikel 3, te weten:
   a. Voor het verkrijgen van inzicht in de mate van gebruik van de elektronisch communicatiemiddelen worden alleen stroom- en soortgegevens vastgelegd;
   b. Voor het voorkomen van onrechtmatig gebruik, dan wel misbruik van de elektronische communicatiemiddelen wordt volstaan met het vastleggen van geanonimiseerde gegevens
   c. Het gebruik op individueel en inhoudelijk niveau wordt slechts gevolgd indien er sprake is van een redelijk vermoeden van onrechtmatig gebruik, dan wel misbruik van de elektronische communicatiemiddelen.

Artikel 9 Persoonsgegevens

1. In de in artikel 8 genoemde vastlegging worden ten hoogste de volgende persoonsgegevens opgenomen:
   a. Gebruikersidentificatie, naam, voornaam of voorletters van de medewerker;
   b. Naam en/of codering van de sector, afdeling waaronder de medewerker valt;
   c. Gegevens over de toegang tot internet die door Regio Rivierenland is geboden aan de medewerker, inclusief gebruikersnaam en internet protocoladres;
   d. Gegevens betreffende de datum en het tijdstip van het openen en sluiten van de toegang tot internet door de medewerker en gegevens betreffende de datum en het tijdstip van het verzenden, dan wel ontvangen van e-mailberichten door de medewerker;
   e. Gegevens, inclusief datum en tijdstip, betreffende de door de medewerker bezochte internetsites (internet protocoladressen en (de onderdelen van) de webpagina's;

2. Indien er een redelijk vermoeden bestaat van onrechtmatig gebruik, dan wel misbruik van de elektronische communicatiemiddelen door medewerker, kan Het Dagelijks Bestuur van Regio Rivierenland opdracht geven om de in het eerste lid, sub e van dit artikel bedoelde gegevens, vast te leggen en te verstrekken aan de personen bedoeld in artikel 11.

Artikel 10 Bewaring en verwijdering

1. De in artikel 9, eerste lid, genoemde persoonsgegevens worden een maand bewaard. Gegevens die ouder zijn dan een maand worden automatisch verwijderd, tenzij er een redelijk vermoeden bestaat van onrechtmatig gebruik, dan wel misbruik van de elektronische communicatiemiddelen in die periode. In dat geval worden de gegevens uit die betreffende maand bewaard zolang dit in het kader van nader onderzoek en eventueel te treffen maatregelen jegens een medewerker noodzakelijk is. Zodra een nader onderzoek is afgerond en dit niet leidt tot maatregelen jegens een medewerker worden de gegevens verwijderd.
2. Indien de systeembeheerder om technische redenen persoonsgegevens als bedoeld in het eerste lid, niet kan verwijderen, wordt onder verwijderen verstaan het niet meer beschikbaar stellen van deze gegevens voor de in artikel 3 geformuleerde doeleinden.

Artikel 11 Personen aan wie persoonsgegevens worden verstrekt

De vastgelegde persoonsgegevens worden, na bewerking, via de secretaris of directeur verstrekt aan:

a. de diensthoofden om inzicht te verkrijgen in de mate van gebruik van de elektronische communicatiemiddelen. Het betreft hier dan slechts de gegevens als bedoeld in artikel 9, eerste lid, sub a tot en met d in niet tot de persoon herleidbare vorm;
b. Het Dagelijks Bestuur van Regio Rivierenland indien er een redelijk vermoeden bestaat van onrechtmatig gebruik dan wel misbruik van de elektronische communicatiemiddelen. Het betreft hier dan de gegevens als bedoeld in artikel 9, eerste lid;
c. degene(n) die op verzoek van Het Dagelijks Bestuur van Regio Rivierenland is (zijn) belast met of leiding geeft (geven) aan onderzoek naar onrechtmatig gebruik dan wel misbruik van de elektronische communicatiemiddelen. Het betreft hier dan de gegevens als bedoeld in artikel 9, eerste lid.

Artikel 12 Rechten van de medewerker

1. De medewerker die daarom verzoekt bij het Dagelijks Bestuur van Regio Rivierenland, ontvangt een overzicht van de hem/haar betreffende persoonsgegevens die worden verwerkt.
2. Indien een gewichtig belang van de verzoeker dit eist, wordt aan dit verzoek voldaan in een andere dan schriftelijke vorm, die aan dat belang is aangepast.
3. Degene aan wie overeenkomstig het eerste lid kennis is gegeven van de hem betreffende persoonsgegevens, kan verzoeken deze te verbeteren, aan te vullen, te verwijderen of af te schermen indien deze feitelijk onjuist zijn, voor het doel of de doeleinden van de verwerking onvolledig of niet ter zake dienend zijn, dan wel anderszins in strijd met een wettelijk voorschrift worden verwerkt.
4. Het verzoek bevat de aan te brengen wijzigingen.
5. Het Dagelijks Bestuur van Regio Rivierenland bericht de verzoeker binnen vier weken na ontvangst van het in het tweede lid genoemde verzoek schriftelijk of, dan wel in hoeverre hij daaraan voldoet. Een weigering is met redenen omkleed. Een beslissing op een verzoek geldt als een besluit in de zin van artikel 1:3, Algemene wet bestuursrecht.
6. Het Dagelijks Bestuur van Regio Rivierenland draagt er zorg voor dat een beslissing tot verbetering, aanvulling, verwijdering of afscherming zo spoedig mogelijk wordt uitgevoerd.

Artikel 13 Sancties

1. Overtreding van deze regeling kan voor medewerkers in dienst van Regio Rivierenland resulteren in disciplinaire maatregelen als bedoeld in artikel 16 CAR-UWO.
2. Regio Rivierenland is gerechtigd om eventuele schade die voor Regio Rivierenland ontstaat door overtreding van deze regeling te verhalen op de medewerker.
3. Overtreding van deze regeling kan voor personen die werkzaamheden voor Regio Rivierenland verrichten, anders dan in ambtelijk dienstverband, resulteren in maatregelen waardoor deze personen, al dan niet tijdelijk, geen beschikking meer hebben over (een deel van) de elektronische communicatiemiddelen. Ook is Regio Rivierenland gerechtigd om eventuele schade die voor Regio Rivierenland ontstaat door overtreding van deze regeling op deze personen te verhalen.

Artikel 14 Onvoorziene omstandigheden

In gevallen waarin deze regeling niet in redelijkheid voorziet beslist het Dagelijks Bestuur binnen de kaders van de CAR-Uwo en de Wbp.

Artikel 15 Citeertitel en inwerkingtreding

Deze regeling kan aangehaald worden als “Regeling gebruik e-mail, internet en social media Regio Rivierenland” en treedt in werking met ingang van de dag na de datum waarop deze regeling bekend

wordt gemaakt, onder gelijktijdige intrekking van het Reglement e-mail en internetgebruik zoals vastgesteld per 1 juni 2004.
De regeling is vastgesteld op 11 mei 2016

Het Dagelijks Bestuur van de Regio Rivierenland

de secretaris,
mevr. mr. I.P.C. van Wamel – Geene
de voorzitter,
de heer R. van Schelven

Artikelsgewijze toelichting Regeling gebruik e-mail, internet en social media Regio Rivierenland

Deze toelichting maakt onlosmakelijk deel uit van de regeling e-mail- en internetgebruik

Vooraf
Binnen organisaties wordt veel gebruikgemaakt van e-mail, internet en andere elektronische communicatiemiddelen. Om het gebruik hiervan in goede banen te leiden, kunnen gedragscodes en gebruiksregels worden opgesteld die door middel van controle worden gehandhaafd. Uit recent onderzoek naar vijf jaar rechtspraak over e-mail- of internetmisbruik blijkt dat de aanwezigheid van een gedragscode zeer relevant is. Het is voor gemeenten en onze organisatie dan ook zaak daarover een duidelijk beleid te voeren. Elektronische controle van computergebruik raakt echter het terrein van de bescherming van de persoonlijke levenssfeer van de medewerker. Op het controleren van het gebruik van e-mail en internet op de werkplek is daarom de Wet bescherming persoonsgegevens (WBP) van toepassing die op 1 september 2001 in werking is getreden.
Het controleren van het gebruik van de e-mail- en internetfaciliteiten is een zogenaamd personeelvolgsysteem. Voor de invoering van een personeelvolgsysteem en een privacyreglement is op grond van artikel 27, eerste lid, onder k en l, van de Wet op de ondernemingsraden, de instemming van de ondernemingsraad (OR) vereist. Dit geldt ook voor een eventuele latere wijziging of bij intrekking van het regeling. Na instemming van de OR kan de regeling op de voor Regio Rivierenland gebruikelijke wijze worden vastgesteld en ingevoerd.
Het Dagelijks Besuur is verplicht om de verwerking van persoonsgegevens te melden bij het College bescherming persoonsgegevens (Cbp) voordat hij begint met de verwerking. In het zogenaamde Vrijstellingsbesluit staan eisen geformuleerd waaraan de verwerkingen moeten voldoen, wil de vrijstelling van de meldingsverplichting daadwerkelijk gelden. Op basis van het Vrijstellingsbesluit valt controle op het gebruik van de e-mail- en internetfaciliteiten onder de vrijstelling mits voldaan wordt aan de vereisten van het Vrijstellingsbesluit. Deze vereisten houden in dat geen andere persoonsgegevens worden verwerkt dan:
a) gegevens ten behoeve van identificatie van en communicatie (username en toegangscode) met de gebruikers binnen het netwerk;
b) gegevens met betrekking tot bevoegdheden van de gebruikers en de netwerkbeheerders met het oog op de aangeboden faciliteiten en diensten van het netwerk;
c) gegevens met betrekking tot de verrichtingen van de gebruikers en netwerkbeheerders;
d) gegevens met betrekking tot elektronische berichten van of voor de gebruikers.

Daarnaast geldt dat de persoonsgegevens slechts worden verstrekt aan degenen die belast zijn met de interne controle en beveiliging (de doeleinden van de verwerking), met dien verstande dat verstrekking aan derden slechts geschiedt met het oog op het behandelen van geschillen. Bovendien dienen de persoonsgegevens uiterlijk zes maanden nadat ze zijn verkregen te worden verwijderd. Ten slotte geldt dat de OR aan de controle instemming heeft verleend.

Artikelsgewijze toelichting
Artikel 1 Begripsbepalingen
De begrippen zoals die in het privacyreglement voorkomen worden hier gedefinieerd. Voor de omschrijving van begrippen is waar mogelijk aangesloten bij de bewoording die wordt gebruikt in de Wbp.
De Wbp is van toepassing als er sprake is van verwerking van persoonsgegevens. Gegevens met betrekking tot het gebruik van de e-mail- en internetfaciliteiten van medewerkers zijn in het algemeen te kwalificeren als persoonsgegevens. IP-adressen zijn in combinatie met de username en het password te herleiden tot een bepaalde gebruiker. De daaraan verbonden bestanden zijn aldus herleidbaar tot een medewerker. De verkeersgegevens geven inzicht in de afzender, de bestemming, de datum en de tijd van het bericht of van het internetgebruik. Ook de inhoud van het e-mailbericht is een persoonsgegeven als de werkgever dit tot zijn beschikking heeft om bijvoorbeeld te controleren of een medewerker de regels in het privacyreglement nakomt. De WBP hanteert een ruime definitie voor het begrip ‘verwerking’: het gehele proces van verzamelen tot aan vernietigen van gegevens.

Artikel 2 Reikwijdte
De regeling is van toepassing op het verwerken van persoonsgegevens inzake het gebruik van e-mail- en/of internetfaciliteiten.
Deze regeling geeft de wijze aan waarop in Regio Rivierenland wordt omgegaan met de e-mail- en internetfaciliteiten en omvat regels ten aanzien van verantwoord gebruik hiervan en regels over de wijze waarop controle hiervan plaatsvindt.
De regeling geldt voor alle medewerkers van de Regio Rivierenland: ambtenaren en personen die (betaald of niet-betaald) werkzaamheden voor de gemeente verrichten, anders dan in ambtelijk dienstverband.

Bestuurders
De regeling is in deze vorm niet van toepassing op leden van het Algemeen en Dagelijks bestuur.

Artikel 3 Doeleinden
De WBP bepaalt dat gegevens in overeenstemming met de wet en op een behoorlijke en zorgvuldige wijze moeten worden verwerkt (artikel 6 WBP). Dit voorschrift geldt in zoverre als de privacyrechtelijke evenknie van de arbeidsrechtelijke norm van goed werkgeverschap. Persoonsgegevens mogen voorts slechts voor welbepaalde, duidelijk omschreven en gerechtvaardigde doeleinden worden verwerkt (artikel 7 WBP). Deze doelomschrijving moet nauwkeurig en zo volledig mogelijk zijn (zie ook artikel 4, eerste lid van de regeling). In overleg moet worden vastgesteld welke doeleinden voor controle van het gebruik van de e-mail- en internetfaciliteiten noodzakelijk zijn voor de eigen organisatie. Controle via volgsystemen is dus alleen toegestaan indien het doel van de controle vooraf is bepaald. Als grondslag van de controle kan doorgaans het gerechtvaardigd belang van de organisatie worden aangewezen (artikel 8, onder sub f WBP). De privacybelangen van de medewerkers horen hierbij dan wel meegewogen te worden. De aard, omvang en vorm van de controlemaatregelen dienen dus in een redelijke verhouding tot het doel van de controle te staan (proportionaliteit), (zie ook artikel 6, eerste lid, onder sub b en de toelichting). Tevens geldt dat de gebruikte controlemiddelen niet meer inbreuk mogen maken op de belangen van de medewerker dan strikt noodzakelijk is (subsidiariteit). In het privacyreglement zijn drie doeleinden geformuleerd.
Controle op het gebruik van de e-mail- en internetfaciliteiten is dus op zichzelf niet verboden. De werkgever is bevoegd om op basis van zijn gezagsbevoegdheid voorwaarden te stellen aan het gebruik van de e-mail-, internet- en overige faciliteiten of bepaalde soorten gebruik te verbieden. De werkgever moet wel de doeleinden bepalen waarvoor hij controle noodzakelijk acht (doelbinding).

Artikel 5 Voorkomen onrechtmatig gebruik dan wel misbruik
Voor het verkrijgen van inzicht in de mate van gebruik van de e-mail- en internetfaciliteiten zal in het kader van kosten- en capaciteitsbeheersing de controle beperkt kunnen blijven tot steekproven. Indien er vanuit de praktijk aanwijzingen of sterke vermoedens bestaan van verkeerd gebruik kan de directeur de teamleider I&A/systeembeheerder opdracht verstrekken.

Artikel 6 Verantwoordelijkheden en beheer
Artikel 4, lid 1
Op de werkgever wordt geen absolute verplichting gelegd. Een garantie voor de juistheid van gegevens kan van de werkgever niet worden gevergd. De juistheid van de gegevens wordt mede bepaald door de context waarin ze worden gebruikt. Met ‘nodige’ maatregelen wordt uitgedrukt dat alle maatregelen moeten worden getroffen die in redelijkheid kunnen worden gevergd. De redelijkheid stelt daarbij, afhankelijk van bijvoorbeeld de soort gegevens die onderwerp van verwerking zijn, de stand van de techniek en de kosten die met de maatregelen gepaard gaan, grenzen aan de te nemen maatregelen.

Artikel 4, lid 2
Deze maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau gelet op de risico’s die de verwerking en de aard van te beschermen gegevens met zich meebrengen. De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen.

Artikel 4, lid 3
Een of meer systeembeheerders zijn met het beheer van de bestanden belast. De systeembeheerder heeft uit hoofde van zijn functie toegang tot alle gegevens in het computernetwerk. De functie van systeembeheerder dient met de nodige waarborgen te worden omgeven. De systeembeheerder moet zich ervan bewust zijn dat hij gegevens die hij tijdens zijn werk tegenkomt, geheim dient te houden. Die verplichting lijdt uitzondering indien enig wettelijk voorschrift hem tot mededeling verplicht of uit zijn taak de noodzaak tot mededeling voortvloeit. De systeembeheerder is uiteraard in beginsel niet bevoegd tot het lezen van documenten of e-mail of het meekijken met het internetgebruik van de medewerkers zonder dat daar een bijzondere aanleiding voor is.
De systeembeheerder dient tegenover het management een zekere onafhankelijkheid te hebben. Er dient dus een heldere procedure te bestaan over wie in welke gevallen de systeembeheerder opdracht kan geven om bepaalde zaken op het netwerk nader te controleren of daarover informatie te verschaffen.

Back-ups
In het kader van zorgvuldigheid zullen regelmatig back-ups van de systemen worden gemaakt die in geval van calamiteiten eenvoudig kunnen worden teruggezet. Dit betekent dat van logbestanden en andere gegevens over het e-mail- en internetgedrag van medewerkers een back-up wordt gemaakt. De werkgever moet zich ervan bewust zijn dat onzorgvuldig of onbevoegd gebruik van deze back-ups even schadelijk kan zijn voor de persoonlijke levenssfeer van de medewerker als onzorgvuldig of onbevoegd gebruik van het actuele systeem. Back-ups dienen daarom op een veilige plaats bewaard te worden. Nadat gegevens zijn aangepast moet zo snel mogelijk een nieuwe back-up gemaakt worden en moeten oude versies worden vernietigd, zodat de gegevens niet na een eventuele terugplaatsing van een back-up nogmaals moeten worden aangepast.

Artikel 7 Gebruik elektronische communicatiemiddelen
In de regeling worden gedragsregels opgenomen over wat er in de organisatie onder verantwoord e-mail- en internetgebruik wordt verstaan. In dit artikel is onder lid 1 een algemene bepaling opgenomen die de bevoegdheid voor het DB creëert om in protocollen nadere regels te stellen over het gebruik van de e-mail- en internetfaciliteiten. In de regeling worden bovendien regels opgenomen over wat niet is toegestaan bij een verantwoord e-mail- of internetgebruik.
Een totaal verbod van privé-gebruik van de e-mail- en internetfaciliteiten is overigens niet mogelijk. Er is een duidelijke uitspraak gedaan over de huidige ‘privétisering’ van de werkplek. Dat houdt in dat een bepaalde mate van niet-zakelijk e-mail- en internetgebruik onder werktijd niet kan worden verboden. (Kantonrechter Haarlem, 16 juni 2000, Jurisprudentie Arbeidsrecht 2000, 170). De werkgever kan wel beperkende voorwaarden opstellen aan het persoonlijk gebruik van de e-mail- en internetfaciliteiten.

Artikel 10 Bewaring en verwijdering
Artikel 10, lid 1
Het is in het algemeen niet nodig om de persoonsgegevens lang te bewaren. De standaardtermijn is daarom maximaal zes maanden. In het geval van een zwaarwegend vermoeden van onrechtmatig gebruik dan wel misbruik van de e-mail- en internetfaciliteiten, worden de gegevens uit die zes maanden bewaard, zolang dit in het kader van nader onderzoek en eventueel te treffen maatregelen jegens een medewerker noodzakelijk is. Zodra een nader onderzoek is afgerond en dit niet leidt tot maatregelen jegens een medewerker worden de gegevens verwijderd.
In relatie tot de termijn gedurende welke persoonsgegevens mogen worden bewaard, kan het volgende worden opgemerkt. De termijn gedurende welke de in archiefbescheiden opgenomen persoonsgegevens mogen worden bewaard, is in beginsel onbepaald. Deze onbepaalde termijn houdt direct verband met het doeleinde waarvoor de gegevens worden bewaard: behoud van (een deel van) het Nederlandse culturele erfgoed.

Artikel 10, lid 2
Bepaalde gegevens kunnen soms om technische redenen niet worden verwijderd. Van het e-mailsysteem worden bijvoorbeeld back-ups gemaakt die in geval van nood teruggezet kunnen worden. Deze back-ups kunnen niet zonder meer gewist worden. Het is ook niet mogelijk om binnen een dergelijke back-up een individueel e-mailbericht te verwijderen. De bedoelde gegevens mogen in deze gevallen niet meer worden verstrekt (verwerkt).

Artikel 11 Personen aan wie controle-informatie wordt verstrekt
Al eerder is opgemerkt dat het controleren op het juiste gebruik op zich niet verboden is volgens de Wbp. Er dient alleen zeer zorgvuldig met het instrument te worden omgegaan. Met het benoemen van een gericht aantal personen die de informatie mogen ontvangen en het benoemen van de weinige opdrachtgevers hiertoe wordt de benodigde zorgvuldigheid vorm gegeven.

Artikel 12 Rechten van de medewerker
In artikel 12 worden de rechten van de medewerkers bij het verwerken van persoonsgegevens behandeld. Transparantie is een belangrijk beginsel voor privacybescherming. De informatieplicht is gebaseerd op de artikelen 33 en 34 WBP.

Artikel 13 Sancties
Tegen het opleggen van disciplinaire maatregelen/straffen kan op basis van de Algemene wet bestuursrecht (Awb) bezwaar en beroep worden aangetekend.

Artikel 14 Onvoorziene omstandigheden
Bij onvoorziene omstandigheden beslist het dagelijks bestuur.